Deteksi *False Alarm* Pada *Intrusion Detection System*(IDS) Menggunakan Algoritma *Adaptive Agent-Based Profiling*

[1)]Jusia Amanda Ginting, [2)] Irwan Sembiring
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50711, Indonesia
Email : [1)] gintingjusia2@gmail.com, [2)] irwan@staff.uksw.edu

Abstract

Network security is important to note, given the large number types of computer attacks. IDS can used as a tool to detect the threats or issued and produce alert consists of alarms and false alarms. False alarms caused by IDS signature patterns that are not good in comparing existing attacks. Reduce the number of false alarms in the IDS can use the algorithms Adaptive Agent-Based Profiling with the purpose to optimize the capabilities of IDS to reduce false alarms in the IDS system. Adaptive algorithms Agent-Based Profiling produce three possibilities: normal behaviour, abnormal behaviour and ambiguous. The conclusion of the research is, the adaptive agent-based algorithm profiling can reduce the number of false alarms by 84% so it can prevent data from overload in IDS.

Keywords *Intrusion Detection System, False Alarm, Adaptive Agent Based Profiling algorithm.*

Abstrak

Keamanan jaringan merupakan hal penting untuk diperhatikan, mengingat banyaknya jenis-jenis serangan komputer. IDS dapat digunakan sebagai *tool* untuk mendeteksi serangan dan mengeluarkan *alert* yang terdiri dari *alarm* dan *false alarm*. *False alarm* disebabkan oleh pola *signature* IDS yang tidak baik dalam membandingkan serangan-serangan yang ada, untuk mengurangi jumlah *false alarm* di dalam IDS dapat menggunakan algoritma *Adaptive Agent-Based Profiling* dengan tujuan untuk mengoptimalkan kemampuan IDS dalam mereduksi *false alarm* di dalam sistem IDS. Algoritma *adaptive agent-based profiling* menghasilkan tiga kemungkinan yaitu: normal *behaviour*, abnormal *behaviour* dan ambigu. Kesimpulan dari penelitian adalah algoritma *adaptive agent-based profiling*, dapat mengurangi jumlah *false alarm* sebesar 84% sehingga dapat mencegah data *overload* pada IDS.

Kata Kunci: *Intrusion Detection System, False Alarm,* Algoritma *Adaptive Agent Based Profiling*

[1)] Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana

[2)] Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana